MATTHEW A. MACDONALD, SBN 255269
TREVOR N. TEMPLETON, SBN 308896
CHRISTOPHER M. HURLEY, SBN 350153
MADELYN Y. CHEN, SBN 346126
WILSON SONSINI GOODRICH & ROSATI
Professional Corporation
953 East 3rd Street, Suite 100
Los Angeles, CA 90013-1952
Telephone: (323) 210-2900
Facsimile: (866) 974-7329
Email: matthew.macdonald@wsgr.com
ttempleton@wsgr.com
churley@wsgr.com
madelyn.chen@wsgr.com

CAITLIN MCKELVIE, *pro hac vice*
WILSON SONSINI GOODRICH & ROSATI
Professional Corporation
95 S. State Street, Suite 1000
Salt Lake City, UT 84111
Telephone: (801) 401-8510
Facsimile: (866) 974-7329
Email: cmckelvie@wsgr.com

Attorneys for Defendant
LIVERAMP HOLDINGS, INC.

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

CHRISTINE RIGANIAN and DONNA SPURGEON, *on behalf of themselves and all others similarly situated,* Plaintiff, v. LIVERAMP HOLDINGS, INC., *a corporation organized under the laws of the State of Delaware,* Defendant.	Case No.: 4:25-cv-824-JST **MOTION TO DISMISS CLASS ACTION COMPLAINT** Before: Hon. Judge Jon S. Tigar Date: June 5, 2025 Time: 2:00 p.m.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

CASES

STATUTES

RULES

NOTICE OF MOTION AND MOTION

PLEASE TAKE NOTICE that, pursuant to Rule 12(b)(6) of the Federal Rules of Civil Procedure, on June 5, 2025 at 2 p.m. or as soon thereafter as this matter may be heard, Defendant LiveRamp Holdings, Inc. ("LiveRamp")[1] will and hereby does move this Court to dismiss Plaintiffs Christine Riganian's and Donna Spurgeon's Class Action Complaint (the "Complaint"). This motion is based on this Notice of Motion and Motion, the accompanying Memorandum of Points and Authorities, all documents in the Court's file, any matter of which this Court may take judicial notice, and on such other written and oral argument as may be presented to the Court. LiveRamp requests that the Court grant its motion and issue an order dismissing Plaintiffs' Complaint in its entirety and with prejudice.

MEMORANDUM OF POINTS AND AUTHORITIES

I. INTRODUCTION

Plaintiffs ask the Court to legislate. If adopted, Plaintiffs' theory would impose sweeping new rules for the online advertising industry and deem illegal longstanding practices that help keep the internet free. This theory finds no support in the law. Worse, it explodes the careful balance that California voters struck in 2020 when they enacted The California Privacy Rights Act ("CPRA") through Proposition 24, a statewide ballot initiative.[2]

That law created detailed rules governing companies that collect, analyze, and store consumer data and added a host of new consumer data rights. Far from banning the collection of consumer information for use in advertising, voters expressly determined that "advertising-supported services … can be a great model for consumers and businesses alike." Prop. 24 § 2(i). Prop 24 created a dedicated privacy agency to pass regulations that "balance" privacy interests with the needs of "business and innovation." *Id.* § 24.7(l). Plaintiffs do not allege that

[1] LiveRamp Holdings, Inc. is a holding company that does not undertake the practices alleged in the Complaint. LiveRamp reserves its rights and defenses.

[2] *See* Proposition 24, The California Privacy Rights Act of 2020 (codified at Cal. Civ. Code Ann. § 1798.100 (West 2025)) (hereinafter "Prop 24") § 2(I), attached as Exhibit B to the Declaration of Trevor Templeton ("Templeton Decl.").

LiveRamp violated any of these rules. Instead, Plaintiffs ask the Court to upend that regime and condemn as "highly offensive" much of what makes targeted advertising work.

According to the Complaint, LiveRamp offers two principal services: (i) "Identity Resolution"—a service, Plaintiffs claim, that allows advertisers to reach their target audiences on digital platforms *without* exchanging personally identifiable information; and (ii) "Data Marketplace"—a platform where third parties are alleged to buy and sell pseudonymized data. Plaintiffs also allege that LiveRamp collects certain information about browsing activity on websites that have chosen to activate a LiveRamp tool, and that it uses this information to facilitate targeted ad delivery. Plaintiffs claim that this routine commercial conduct violates Plaintiffs' privacy rights, the California Invasion of Privacy Act ("CIPA"), and the Electronic Communications Privacy Act of 1986 ("ECPA"), and that LiveRamp has been unjustly enriched. Each of these claims fails as a matter of law.

First, Plaintiffs' common law and constitutional claims (Counts I and II) fail because Plaintiffs have not (i) plausibly alleged either that they had a reasonable expectation of privacy in their identifying information or internet activities, or (ii) cleared the "high bar" of pleading that any intrusion was "highly offensive." Courts have long recognized that users of the internet have limited expectations of privacy. Here, there is no allegation that LiveRamp (or any of its customers) made misrepresentations about the data it was collecting or how it would be used. LiveRamp is not plausibly alleged to have engaged in "comprehensive" tracking of users' internet activity; rather, LiveRamp's cookies are alleged to be installed only on select customers' websites. None of the information that LiveRamp allegedly collected about Plaintiffs can fairly be called "sensitive." LiveRamp's conduct is nothing more than "routine commercial behavior," that is not actionable. *See Folgelstrom v. Lamps Plus, Inc.*, 195 Cal. App. 4th 986, 992 (2011). Further, to the extent Plaintiffs' claims arise out of the operation of Data Marketplace, those claims are barred by Section 230 of the Communications Decency Act (among other reasons).

Second, Plaintiffs' ECPA and CIPA wiretapping claims (Counts III and IV) fail because Plaintiffs have not plausibly alleged that LiveRamp "intercepts" any communication while it is "in transit." *See Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 876 (9th Cir. 2002). To plead

this claim, Plaintiffs must plausibly allege that LiveRamp's pixels intercept the contents of their communications with partner websites before those communications reach the websites' servers. Plaintiffs plead no such facts but instead rely improperly on conclusory allegations that merely parrot the elements of the cause of action. Plaintiffs' ECPA claim fails for the additional, independent reason that the ECPA is a one-party consent statute, and Plaintiffs do not allege that LiveRamp's tracking pixels were placed on any website without that website owner's consent.

Third, Plaintiffs' CIPA pen register claim (Count III) fails because the statute applies to devices that record *telephonic* activity, not to software that collects information about web browsing activity. This CIPA provision is a penal statute which must be narrowly construed. There is no indication in the statutory text or the legislative history that the Legislature intended it to cover anything other than traditional phone activity. For this reason, multiple California courts have held that the pen register statute does not apply to the technology at issue here.

Finally, Plaintiffs' standalone claim for unjust enrichment (Court V) fails to plead any quasi-contract and is therefore barred by controlling Ninth Circuit authority. And because all of Plaintiffs' other claims fail, so does their claim for declaratory relief (Count VI).

II. BACKGROUND

A. LiveRamp's Services

LiveRamp is a technology company and registered data broker. (Compl. ¶ 39.) It primarily provides services that enable advertisers to deliver targeted ads across digital platforms, a function that helps keep the internet free. *See* Prop 24 § 2(I). LiveRamp's business is heavily regulated by California agencies, Prop 24, and other related laws. California's laws in this regard adopt an opt-out approach, rather than requiring affirmative consent or prohibiting data collection. *See* Cal. Civ. Code §§ 1798.100, 1798.115, 1798.120, 1798.121.

Though the Complaint repeatedly acknowledges the existence of this legal regime (*e.g.*, Compl. ¶¶ 118, 125-127), Plaintiffs do not allege that LiveRamp violated any of these laws or regulations. Nevertheless, Plaintiffs' prolix complaint broadly characterizes LiveRamp as a "Privacy Death Star" that enables a "massive" and unlawful "identity surveillance system." (*Id.* ¶¶ 1, 3, 55.) Plaintiffs' allegations focus on two "principal services" that LiveRamp offers,

namely "Identity Resolution" and "Data Marketplace." (*Id.* ¶ 56.) In describing these services below, LiveRamp accepts (as it must) the truth of the well-pleaded factual allegations of the Complaint but notes for the record its vigorous disagreement with many of those allegations.

Identity Resolution. Identity Resolution improves the process of targeted ad delivery by allowing advertisers to reach customers across different platforms. Consider an advertiser (*e.g.*, a shoe company) that wants to reach identified customers when they visit another website that sells advertising space (*e.g.*, a news website). Identity Resolution works to match the customers on the shoe company's list with visitors to the news website. (*See id.* ¶¶ 82 *et. seq.*)

This process works by assigning an individual an identifier called a "RampID"—pseudonymous identifiers consisting of strings of alphanumerical characters that are meaningless to a human reader. (*See id.* ¶¶ 1, 3, 56, 57.) LiveRamp allegedly constructs RampIDs by collecting both offline and online data about individuals. (*Id.* ¶ 57.) The offline data consists of basic information like names, emails, addresses, driver's license data and social security numbers. (*Id.* ¶¶ 57, 63-68.)[3] According to Plaintiffs, LiveRamp uses software to "infer[] connections" between different offline identifiers and can consolidate them into a RampID. (*Id.* ¶¶ 3, 17, 58, 64 70). The Complaint does not allege that the manner of the collection of this data is unlawful. In fact, Plaintiffs acknowledge that LiveRamp collects this information from "public record data, publicly available data, and self-reported information." (*Id.* ¶ 64 (cleaned up).)

The "online" identifiers consist of information LiveRamp obtains from "partner" websites, such as Google, allegedly by using common software tools such as Client-Side Tags, Web Match Tags, JavaScript code, and pixels. (*Id.* ¶¶ 71, 72, 75-78.) Online identifiers include cookie IDs, mobile IDs, and other identifiers tied to specific browsers or devices. LiveRamp allegedly consolidates these online identifiers with RampIDs to create an "identity graph," such

[3] Plaintiffs allege that the creation of a RampID begins with the "AbiliTec system," which links public record data, publicly available data, and self-reported information" into "AbiliTec IDs." (*Id.* ¶ 64.)

that a single RampID might stand in for multiple offline and online identifiers associated with one person. (*Id.* ¶¶ 71, 79.)

Plaintiffs also allege that Identity Resolution includes the collection of information about individuals' internet browsing history. Specifically, Plaintiffs allege that for those websites on which its "Client-Side Tags" are installed, LiveRamp captures information such as pages viewed, additions to shopping carts, and "segment" and "category" information for products viewed, and then incorporates that information into individual profiles. (*Id.* ¶¶ 23-25, 77.)

Though the Complaint liberally uses words like "manipulation" and "surveillance," LiveRamp is not alleged to be doing any of this out of curiosity or prurient interest. Rather, LiveRamp is alleged to be performing these tasks to help advertisers reach prospective customers across different advertising platforms. (*Id.* ¶¶ 82-87.)

Plaintiffs do not allege that these processes result in the sharing of *any* identifying personal information. To the contrary, Plaintiffs concede that RampIDs are *pseudonymized* (*id.* ¶¶ 3, 89), meaning they cannot be tied to identifiable people without additional information. Indeed, conclusory assertions aside (*see, e.g.*, *id.* ¶ 57), Plaintiffs do not allege that *anyone* has ever de-pseudonymized (or de-anonymized, as they refer to it) a RampID to identify a person tied to the RampID. Plaintiffs do not allege that RampIDs provide any identifiable personal information to the advertisers, digital platforms, or others. In fact, documents cited in the Complaint reveal the opposite: LiveRamp uses multiple security measures to "ensure [that] RampIDs cannot be directly tied back to PII." (*Interpreting RampID, LiveRamp's People-Based Identifier*, LIVERAMP, https://docs.liveramp.comIconnectienlinterpreting-rampid,-liveramp-s-people-basedidentifier.html [https://perma.cc/LC62-K3V2] (quoted at Compl. ¶ 6, n.3).)

Data Marketplace. The second "principal service[]" identified in the Complaint is Data Marketplace. (Compl. ¶¶ 93-106.) Data Marketplace is a platform that enables third-party buyers and sellers—such as TransUnion and Experian—to access and share consumer data for advertising purposes. (*Id.* ¶¶ 94-96.) The Complaint provides no well-pleaded allegation that *LiveRamp itself* buys or sells any data on Data Marketplace. Rather, LiveRamp's alleged role is limited to providing the platform that other companies use for these transactions. (*Id.* ¶ 101.)

Although Plaintiffs allege that there are or were "sensitive" segments available for sale by third parties on the Data Marketplace (*id.* ¶¶ 96-97), Plaintiffs do not allege any facts concerning how those segments were constructed or how the data was collected. For example, Plaintiffs describe segments about "poor people" (*id.* ¶ 96) but do not allege that this segment was constructed with sensitive financial data rather than algorithmically (for example, with zip code information). Similarly, Plaintiffs describe segments about users of "Grindr," but they fail to make any allegation about what notice, consent, or choice may have been given for the collection or sharing of the underlying data or whether people in that segment are sensitive about disclosing that information. Moreover, Plaintiffs do not allege that *they* are in any sensitive segment. Nor is there any allegation that anyone ever de-pseudonymized any of this allegedly sensitive data obtained on Data Marketplace to tie that information to a person's offline identity.[4]

B. The Plaintiffs

Plaintiffs Riganian and Spurgeon are residents of California and Oregon, respectively, who claim to be "concerned citizens" who have been "surveilled" by LiveRamp. (Compl. ¶ 12.) Plaintiffs do not allege that LiveRamp violated any of their rights under the consumer protection statutes that their states have enacted to regulate the data broker industry. Nor do they allege that LiveRamp lied to them or misrepresented any fact about its alleged use of their information.

Plaintiffs each requested and received a Subject Access Request ("SAR") report from LiveRamp. (*Id.* ¶¶ 14, 30.) The SAR reports allegedly show the "information LiveRamp [has] collected and processed" about each of the named Plaintiffs. (*Id.*) These reports purportedly contain, among other things, addresses where Plaintiffs have lived, emails they used, and online identifiers assembled about them. (*Id.*) SAR reports are requested and prepared in compliance with California law, Cal. Civil Code § 1798.110(a), and there are no allegations that LiveRamp would have maintained such a document absent an express request from a consumer.

Tellingly, Plaintiffs fail to allege what sensitive information might be gleaned from their online activity as reflected in the SAR. Plaintiff Riganian alleges she visited the LA Times

[4] We address Plaintiffs' allegations about Third-Party Data Attribute Append below.

website, general health information websites, hulu.com, a bank website, and that she browsed for antacids on cvs.com. (*Id.* ¶¶ 22-27.) Plaintiff Spurgeon alleges she visited general health information websites, cvs.com, showtime.com, news websites, and svu.edu. (*Id.* ¶¶ 36-38.)

Further, and although Plaintiffs acknowledge that the internet is awash in disclosures about data collection practices and that many websites use cookie pop ups that require opt-in consent (*id.* ¶¶ 135-138), Plaintiffs allege that they did not consent to LiveRamp's collection of data. (*Id.* ¶¶ 129-143.) Their theory is not that the websites they visited failed to disclose the collection or sale of data or that LiveRamp misled them. They do not allege that they exercised their opt-out rights or that LiveRamp failed to honor those rights. Rather, their claim is that the internet has become so important that it is unfair even to ask for consent (*id.* ¶ 130), that there are so many disclosures available that Plaintiffs cannot be asked to read and understand them all (*id.* ¶¶ 135, 137), and thus that *no* consent (whether opt-out or opt-in) could ever be effective.

C. Plaintiffs' Legal Claims

Plaintiffs assert six causes of action: (1) invasion of privacy under the California constitution; (2) intrusion upon seclusion under California common law; (3) violations of CIPA (both for wiretapping and for operating a "pen register"), Cal. Penal Code §§ 630 *et seq.*; (4) violations of ECPA, 18 U.S.C. § 2510 *et seq.*; (5) unjust enrichment; and (6) declaratory and injunctive relief. Arguing that California law should apply to their intrusion upon seclusion and unjust enrichment claims on behalf of a nationwide class (Compl. ¶¶ 167, 239), Plaintiffs seek to represent four different classes that include all adult United States or California consumers (1) whose "personal information" was "made available for sale or use" to LiveRamp customers, or (2) who had the contents of their electronic communications "intercepted" by LiveRamp tracking software. (*Id.* ¶ 144.)

III. LEGAL STANDARD

To survive a motion to dismiss, a complaint must contain sufficient factual matter, accepted as true, to "state a claim to relief that is plausible on its face." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). "[A] sheer possibility that a defendant has acted unlawfully" is not enough. *Id.* Courts do not assume the truth of legal conclusions pleaded as factual allegations;

nor do they accept as true allegations contradicted by judicially noticeable facts. *Id.* at 677-79; *Bell Atl. v. Twombly*, 550 U.S. 544, 555 (2007) (plaintiff must plead "more than labels and conclusions, and a formulaic recitation of the elements of a cause of action will not do").

IV. ARGUMENT

A. The Complaint Fails to State an Invasion of Privacy Claim (Counts 1 & 2).

Successfully pleading a claim for a privacy intrusion in California requires a plaintiff to clear a "high bar." *Low v. LinkedIn Corp.*, 900 F. Supp. 2d 1010, 1025 (N.D. Cal. 2012); *In re Google Assistant Priv. Litig.*, 457 F. Supp. 3d 797, 830 (N.D. Cal. 2020). "Actionable invasions of privacy must be sufficiently serious in their nature, scope, and actual or potential impact to constitute an egregious breach of the social norms underlying the privacy right." *Hill v. Nat'l Collegiate Athletic Assn.*, 7 Cal. 4th 1, 37 (1994). Because California's constitutional privacy cause of action and the tort of intrusion upon seclusion have virtually identical elements, "courts consider the claims together and ask whether: (1) there exists a reasonable expectation of privacy, and (2) the intrusion was highly offensive." *In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589, 601 (9th Cir. 2020). Plaintiffs satisfy neither of these requirements. The courts have long recognized that, because of the nature of the internet, its users have limited reasonable expectations of privacy. And Plaintiffs' claims that LiveRamp's conduct was "highly offensive" are in fundamental tension with the decisions of the voters and the California Legislature, who have both endorsed disclosure and the opt-out process as the appropriate way to balance regulation of data collection on the internet.

1. Plaintiffs Fail to Allege a Reasonable Expectation of Privacy.

Plaintiffs have not plausibly alleged that LiveRamp's conduct violated their reasonable expectations of privacy. When determining whether a reasonable expectation of privacy exists, "courts consider a variety of factors, including the customs, practices, and circumstances surrounding a defendant's particular activities." *Facebook*, 956 F.3d at 601-02. The analysis considers both the sensitivity of the information and "whether the manner it was collected . . . violates social norms." *Id.* at 603. "[I]f the allegations show no reasonable expectation of privacy or an insubstantial impact on privacy interests," the claim may be dismissed "as a matter

of law." *Low*, 900 F. Supp. 2d at 1025 (cleaned up); *Hammerling v. Google LLC*, 615 F. Supp. 3d 1069, 1089 (N.D. Cal. 2022).

To begin, LiveRamp's alleged compilation of *offline* "identifiers" (names, addresses, emails, and the like (*see* Compl. ¶¶ 14(a)-(b), 30(a)-(b)), does not violate Plaintiffs' reasonable expectation of privacy any more than the compilation of similar information in a phone book or web directory would. Contact information is not confidential; it is "designed to be exchanged to facilitate communication and is thus available through ordinary inquiry and observation." *I.C. v. Zynga, Inc.*, 600 F. Supp. 3d 1034, 1049 (N.D. Cal. 2022). Thus, the collection and use of names, emails, and similar identifiers does not violate Plaintiffs' reasonable expectation of privacy. *Id.*; *see also Cabral v. Supple, LLC*, 2012 WL 12895825, at *3 (C.D. Cal. Oct. 3, 2012); *Belaire-West Landscape, Inc. v. Super. Ct.*, 149 Cal. App. 4th 554, 561 (2007).

LiveRamp's alleged collection of driver's license and social security numbers (Compl. ¶¶ 17, 32) is no different. Plaintiffs do not allege that the *manner* in which LiveRamp obtained these—or any other offline identifier—was wrongful or violated social norms. To the contrary, they allege that LiveRamp obtained the information from "public record data, publicly available data, and self-reported information." (*Id.*¶ 64 (cleaned up)). Obtaining information that is public record, or that Plaintiffs have self-reported, does not violate any reasonable expectation of privacy. Indeed, courts have recognized that "the interests in privacy fade when the information involved already appears in the public record." *See Cox Broad. Corp. v. Cohn*, 420 U.S. 469, 494–95 (1975); *see also Zynga*, 600 F. Supp. 3d at 1049 ("[T]there is no liability for giving publicity to facts about the plaintiff's life that are matters of public record …." (quoting Restatement (Second) of Torts § 652D, Comment b)). LiveRamp is aware of no case holding that the mere *assembly* of such information can give rise to liability.

Nor have Plaintiffs alleged that they have a reasonable expectation of privacy in the *online* information that LiveRamp collects. "Generally, the internet is not a place where users have a reasonable expectation of privacy." *Thomas v. Papa Johns Int'l, Inc.*, 2024 WL 2060140, at *1 (S.D. Cal. May 8, 2024). "Given the inherent nature of the internet, a number of courts have found that consumers do not have a reasonable expectation of privacy over their activity in

that space." *Id.* at *2 (collecting cases); *see also Farst v. AutoZone, Inc.*, 700 F. Supp. 3d 222, 230 (M.D. Pa. 2023) ("Shopping on a public website, like shopping in a public store, is not an activity one can reasonably expect to keep private from the retailer."). After all, "in this age of information sharing and inter-connectivity, most of us understand that what we do on the internet is not completely private." *State v. Mixton*, 250 Ariz. 282, 293 (2021) (cleaned up). Only "the dissemination or misuse of *sensitive* and *confidential* information" is protected. *In re Yahoo Mail Litig.*, 7 F. Supp. 3d 1016, 1041 (N.D. Cal. 2014) (emphasis added). None of the data at issue here qualifies.

Digital identifiers associated with Plaintiffs—IP addresses, "cookies," "unique device identifiers," etc. (Compl. ¶¶ 14(c)-(e), 30(c)-(e))—do not qualify. *See Heeger v. Facebook*, 509 F. Supp. 3d 1182, 1189 (N.D. Cal. 2020) (finding no "legally protected privacy interest in IP addresses"); *United States v. Forrester*, 512 F.3d 500, 510 (9th Cir. 2008) (finding that "e-mail and Internet users have no expectation of privacy in the to/from addresses of their messages or the IP addresses of the websites they visit"); *Massie v. Gen. Motors LLC*, 2022 WL 534468, at *5 (D. Del. Feb. 17, 2022) ("Plaintiffs fail to explain how [Defendants'] possession of anonymized, non-personal data regarding their browsing activities on GM's website harms their privacy interests in any way."); *see also Saeedy v. Microsoft Corp.*, 2023 WL 8828852, at *4 (W.D. Wash. Dec. 21, 2023) (holding that "mouse movements, clicks, keystrokes, keywords, URLs of web pages visited, product preferences, interactions on a website, search words typed into a search bar, user/device identifiers, anonymized data, product selections added to a shopping cart, and website browsing activities" are not private).

As for browsing histories, Plaintiffs plead no facts suggesting there was anything sensitive about their interactions with websites where they were allegedly tracked. *See Low*, 900 F. Supp. 2d at 1025 (holding web users had no reasonable expectation of privacy in URLs that, in aggregate, disclosed their browsing history on a social media platform). The handful of websites or webpages alleged to have LiveRamp "tracking mechanisms"—healthline.com, cvs.com, abcnews.go.com, and the like (Compl. ¶¶ 26, 37)—are hardly the type that courts have found to count as "sensitive." At most, Plaintiffs say that Riganian viewed a product listing for a

common, over-the-counter antacid on cvs.com. (Compl. ¶¶ 22.) As a matter of law, this is not the kind of "sensitive" information that can create an expectation of privacy. *See Smith v. Facebook, Inc.*, 745 Fed. Appx. 8, 9 (9th Cir. 2018) (browsing for publicly available health information is not "so sensitive" because doing so "cannot, in and of itself, reveal details of an individual's health status or medical history); *see also Smith v. Facebook, Inc.*, 262 F. Supp. 3d 943, 954–55 (N.D. Cal. 2017) (explaining that web pages "contain[ing] general health information" are not "protected health information" because they do not relate to "the past, present, or future physical or mental health or condition of an individual" (citation omitted)).

Neither do Plaintiffs suggest that any website listed in the Complaint collected or shared their information in violation of an applicable privacy policy. For example, although Riganian complains about LiveRamp allegedly receiving a cvs.com URL, she does not allege that CVS promised to keep this information secret. CVS's privacy policies state the opposite.[5] LiveRamp itself publicly discloses how its services work; after all, Plaintiffs drafted their lengthy complaint by summarizing (and mischaracterizing) dozens of LiveRamp's own public disclosures. (*See, e.g.*, Compl. ¶¶ 2-4, 44- 50, 52-59, 61, 64-67.) These disclosures confirm the absence of any reasonable expectation of privacy in Plaintiffs' interactions with the websites they claim to have visited. *See Hammerling v. Google, LLC*, 2024 WL 937247, at *3 (9th Cir. Mar. 5, 2024) ("[T]he Policy here expressly disclosed Google's intention to track their activity on third-party apps. As a result, Plaintiffs have no reasonable expectation of privacy in that data.").

Nor can Plaintiffs invoke *Facebook* to argue that the *aggregation* of individually unprotected information creates an expectation of privacy. There, after expressly promising not to, Facebook tracked logged-out users *everywhere* they went online and then consolidated that information with information-rich Facebook profiles. *Facebook*, 956 F.3d at 599, 603, 606 n.8. The stark differences between this case and *Facebook* underscore the flaws in Plaintiffs' case:

[5] CVS's Privacy Policy expressly discloses that it collects (among other things) "the areas or pages of our Services that you visit" and "items placed or left in your shopping cart on the Site" and that it shares data with third parties. CVS Pharmacy, *Privacy Policy*, https://www.cvs.com/retail/help/privacy_policy (last visited Mar. 15, 2025). The other cited websites have similar policies. *See, e.g.*, GoodRx, *Privacy Policy*, https://www.goodrx.com/about/privacy-policy (last visited Mar. 18, 2025).

(1) The disclosures are different: In *Facebook*, the "critical fact" was that Facebook "affirmatively stated that logged-out user data would not be collected" and thus had itself "set an expectation" of privacy that might not otherwise exist. 956 F.3d at 602-03.[6] Here, there is no such allegation. In fact, Plaintiffs acknowledge that copious disclosures exist online about both LiveRamp's and its customers' data collection practices. Plaintiffs avoid including the contents of any such disclosures. (Compl. ¶¶ 137-139.)[7] The reason is obvious: the disclosures clearly say that the websites will collect and share information with third parties like LiveRamp.

(2) The "amount of data" is different: In *Facebook*, plaintiffs alleged that Facebook tracked them *everywhere* they went, across *seven million* websites. 956 F.3d at 596, 603. Here, LiveRamp's Client-Side Tags are alleged to collect data from "hundreds" of websites—approximately one *ten thousandth* the number at issue in Facebook. (Compl. ¶¶ 35, 84.)

(3) The "nature" of the data is different. In *Facebook*, the defendant collected a "*comprehensive* browsing history of an individual, *no matter how sensitive the website visited* …." 956 F.3d at 603 (emphasis added). Here, Plaintiffs list only a handful of specific websites that allegedly contained LiveRamp "tracking mechanisms." (Compl. ¶¶ 25, 35, 84.) Although Plaintiffs repeatedly assert that these select websites are "sensitive," the only *facts* that Plaintiffs plead are that the websites relate to general health information or articles about "personal financial issues." (*Id.* ¶¶ 20, 35.) These allegations are far too vague and conclusory to clear the "high bar" of pleading a plausible invasion of privacy claim.

(4) The "correlat[ions]" are different. Facebook was alleged to "correlate" browsing history with "personal Facebook profiles," which could include information such as a user's "employment history and religious affiliations." 956 F.3d at 599. LiveRamp is not alleged to

---

[6] Indeed, such a misrepresentation is the "critical fact" in virtually every case to have found a reasonable expectation of privacy in online activity. *See, e.g.*, *In re Nickelodeon Consumer Privacy Litig.*, 827 F.3d 262, 266 (3d Cir. 2016); *In re Google Inc.*, 806 F.3d 125 (3d Cir. 2015); *Hart v. TWC Prod. & Tech. LLC*, 526 F. Supp. 3d 592, 605 (N.D. Cal. 2021) (Tigar, J.) (defendant falsely represented that it would limit use of geolocation data).

[7] Plaintiffs complain that LiveRamp's privacy policies do not mention the Data Marketplace (¶ 146), but of course LiveRamp's privacy notice plainly discloses that it sells certain categories of data and information about the Data Marketplace is readily publicly available. https://liveramp.com/privacy/california-privacy-notice/; https://liveramp.com/data-marketplace/.

have anything remotely resembling a Facebook profile—where users post photos, identify friends and family, share interests and "likes." Moreover, the Complaint acknowledges that information with LiveRamp is pseudonymized, and there are no well-pleaded allegations that anyone has ever de-pseudonymized data such that browsing history or interests can be "correlated" to an identifiable person. Courts recognize that sharing information about internet users that does not disclose their offline identity does not invade a reasonable expectation of privacy. *Zynga*, 600 F. Supp. 3d at 1049 (dismissing invasion of privacy claim based on data breach when plaintiffs' "anonymity is preserved"); *see Sanchez v. Los Angeles Dep't of Transp.*, 2021 WL 1220690, at *3 (C.D. Cal. Feb. 23, 2021) ("Obviously, a person does not have a reasonable expectation of privacy over information that cannot even be connected to her.").

Katz-Lacabe v. Oracle America, Inc., 668 F. Supp. 3d 928 (N.D. Cal. 2023), doesn't help Plaintiffs either. That case—filed by the same lawyers representing Plaintiffs here—involved claims against Oracle, which provided identity resolution services and a data marketplace. The court denied Oracle's motion to dismiss but held that it was a "close question" as to whether the plaintiffs had alleged enough detail to plausibly state a claim based on aggregation of data. *Id.* at 942. There is no close question here. Oracle collected browsing data from 48,000 websites, not several hundred. (*Compare* Oracle Compl. ¶ 38,[8] *with* Compl. ¶¶ 20, 35, 59.) Oracle was able to collect data sufficient to infer whether a "person isn't sleeping well, or is experiencing headaches or sore throats, or is looking to lose weight, and thousands of other invasive and highly personalized inferences." (Oracle Compl. ¶ 49(b); *see also id.* ¶¶ 28-37, 50-73.) Plaintiffs even cited Oracle's own statements that Oracle was *better* than Facebook at predicting user behavior. (*Id.* ¶ 55; *see also id.* ¶¶ 49, 59, 61 (alleging Oracle's creation and sale of segments that "develop inferences about specific people" and "reveal sensitive, health-related" information and track everything about them from "where they live, to the media they consume, to the things they buy, [and] to the views they hold").) Plaintiffs' allegations against LiveRamp do not come close.

[8] ECF No. 1, No. 3:22-cv-04792-SK, 2022 WL 22867093 (N.D. Cal. Aug. 19, 2022).

Plaintiffs' equivocal allegations about a product called Third Party Attribute Data Append ("Attribute Append") do not cure their problem. Plaintiffs suggest that this product "appears" to allow companies to scrape data from Data Marketplace and then attach it to pre-existing PII about individuals. (Compl. ¶¶ 107-10.) As an initial matter, Plaintiffs' allegations about this product are based entirely on their gross misinterpretation of a LiveRamp publication that they incorporate by reference titled *Third-Party Attribute Data Append*. (Compl. ¶ 107 n.102.)[9] The sentence they rely on says something very different: that Live Ramp generates a "*fill rate report* for all the currently-available data seller attributes and shares *that*" (the fill rate report). Nothing about the document says that the "available" attributes include every attribute that can be found on Data Marketplace. Because the allegation is contradicted by Plaintiffs' own cited documents, the Court may disregard it. *See Sprewell v. Golden State Warriors*, 266 F.3d 979, 988 (9th Cir. 2001). In any event, because Plaintiffs couched their allegation in equivocal language (it "appears"), it should receive no consideration. *See Sachsenberg v. IRSA Inversiones Y Representaciones Sociedad Anónima*, 339 F. Supp. 3d 169, 181 (S.D.N.Y. 2018) ("equivocal allegations are insufficient to state a claim"); *Little v. Quality Title Servs., LLC*, 2023 WL 7086450 (E.D. La Oct. 26, 2023). That is doubly true where Plaintiffs never allege LiveRamp actually *de*-pseudonymized any sensitive data. (*See e.g.*, Compl. ¶¶ 107-10.)

2. Plaintiffs Fail to Allege Any "Highly Offensive" Invasion.

Even if Plaintiffs had a reasonable expectation of privacy in the information LiveRamp allegedly compiled, they have not plausibly alleged the intrusion was "highly offensive." An invasion of privacy is highly offensive only if it is "sufficiently serious in [its] nature, scope, and actual or potential impact to constitute an egregious breach of the social norms underlying the privacy right." *Low*, 900 F. Supp. 2d at 1025 (citation omitted). The Ninth Circuit has described that as requiring an "*exceptional* kind of prying into another's private affairs" akin to "taking the photograph of a woman in the hospital with a 'rare disease that arouses public curiosity'" or

[9] The document is available at the permalink referenced at footnote 102 of the Complaint and at the following URL: https://docs.liveramp.com/connect/en/offline-data-marketplace.html.

"using a telescope to look into someone's upstairs bedroom window for two weeks and taking 'intimate pictures.'" *Med. Lab'y Mgmt. Consultants v. Am. Broad. Companies, Inc.*, 306 F.3d 806, 819 (9th Cir. 2002). The issue can be decided at the pleadings. *Hubbard v. Google LLC*, 2024 WL 3302066, at *7 (N.D. Cal. July 1, 2024); *Thomas*, 2024 WL 2060140 at *6.

There is no allegation that LiveRamp collected specific types of information that are so sensitive that collecting them is an "egregious breach" of social norms. *Low*, 900 F. Supp. 2d at 1025 (citation omitted). Allegedly collecting a URL showing Riganian viewed an over-the-counter antacid, (Compl. ¶ 22), is not remotely like photographing a hospital patient with a rare disease or taking "intimate pictures" through a bedroom window. *See Med. Lab'y*, 306 F.3d at 819; *Folgelstrom*, 195 Cal. App. 4th at 991-92 (describing "dissemination of photographs of [a] decapitated corpse" and "gratuitous disclosure of a patient's HIV status" as representative of highly offensive intrusions). Indeed, this alleged conduct is substantially less invasive than collecting a plaintiff's online searches for medical providers, which was deemed insufficient to state a claim in *Cousin v. Sharp Healthcare*, 681 F. Supp. 3d 1117, 1124 (S.D. Cal. 2023).[10]

Also absent is any allegation that LiveRamp disclosed facts about Plaintiffs in a highly offensive manner. Under the high bar established by California law, "[e]ven disclosure of personal information, including social security numbers, does not constitute an 'egregious breach of the social norms' …." *Low*, 900 F. Supp. 2d at 1025 (citation omitted).[11] Plaintiffs plead no facts showing that LiveRamp disclosed anything sensitive about them to a third party in a way that caused embarrassment or injury. To the contrary, Plaintiffs acknowledge that LiveRamp consolidates personal identifying information into pseudonymized RampIDs. (Compl. ¶¶ 3, 82, 89.) Courts "have consistently refused to characterize the disclosure of common, basic digital information to third parties as serious or egregious violations of social norms." *In re Google,*

[10] Nor have Plaintiffs alleged that LiveRamp collects precise geolocation data. *Cf. Greenley v. Kochava, Inc.*, 684 F. Supp. 3d 1024 (S.D. Cal. 2023).

[11] *See also In re iPhone App. Litig.*, 844 F. Supp. 2d 1040, 1063 (N.D. Cal. 2012) (disclosure of "unique device identifier number, personal data, and geolocation information"); *Google Privacy Policy*, 58 F. Supp. 3d at 973-74 (disclosure of names, private contact lists, and contents of email communications); *McCoy v. Alphabet, Inc.*, 2021 WL 405816, at *8 (N.D. Cal. Feb. 2, 2021) (disclosure of app usage data).

Inc. Privacy Policy Litig., 58 F. Supp. 3d 968, 985 (N.D. Cal. 2014). Setting aside Plaintiffs' allegations about Attribute Append, *supra* at 14, there is no well-pleaded allegation that LiveRamp has ***ever*** pierced pseudonymization by communicating digital identifiers together with information that could be associated with an identifiable person. *See Zynga*, 600 F. Supp. 3d at 1049 (no highly offensive intrusion absent disclosure of personally identifiable information). Mere speculation that this could *theoretically* happen is insufficient to state a claim. *See Cousin*, 681 F. Supp. 3d at 1126 (conduct not highly offensive because even if the data "*could* be de-anonymized," there was no allegation that "anyone has *actually done so*" (emphases added)).

Moreover, for the reasons stated above (*see supra* at p.14), *Facebook* is inapposite. Plaintiffs have failed to allege the "critical fact" behind *Facebook*—false representations about the scope of data collection. Indeed, the privacy policies for the websites that Plaintiffs claim to have visited disclose data collection and sharing. *See Hammerling*, 2024 WL 937247, at *3 (no highly offensive intrusion when policies disclosed collection). LiveRamp similarly publicly discloses its activity. Further, and unlike in *Facebook*, Plaintiffs do not allege that LiveRamp internally acknowledged that its conduct was wrongful. *Cf. Facebook*, 956 F.3d at 606.

LiveRamp's alleged conduct amounts to only legally permissible "routine commercial" practice in support of ad delivery, which requires dismissal of Plaintiffs' claim. *See Folgelstrom*, 195 Cal. App. 4th at 992. In *Folgelstrom*, the court affirmed dismissal of a consumer's invasion of privacy claim against an advertiser that surreptitiously collected their home address information and used that information to send targeted ads. *Id.* at 989-92. The court reasoned that even if the information was obtained through "questionable" means, no claim would lie unless the information was *used* in a highly offensive way. *Id.* at 993. Because the advertiser used the information to determine where to send the consumer advertising, the conduct was not highly offensive as a matter of law, and the privacy claim was properly dismissed. *Id.*

Similarly, in *Hubbard v. Google LLC*, the court dismissed the plaintiffs' privacy torts for failure to plead that Google's collection of their online "cookies and persistent identifiers" was highly offensive. 2024 WL 3302066, at *7. Google allegedly collected detailed information about the minor plaintiffs' online browsing activity, including their "searches run, videos

watched," "purchase activity," "browsing history," and "device sensor data." *Id.* at *2. Nonetheless, the court dismissed plaintiffs' invasion of privacy claims on the ground that this data collection was routine commercial behavior. *Id.* at *7. The court distinguished *Facebook* and other cases that found actionable privacy invasions online because the case did not involve "secret or deceptive data collection" or "the misappropriation of data stemmed from a data breach." *Id.* & n.9. The court reasoned that "[w]ithout any such 'plus factors' … to elevate Defendants' conduct beyond the level of routine commercial behavior, Plaintiffs effectively ask the Court to characterize an entire industry as founded on tortious conduct. The Court cannot sanction that result." *Id.* at *7. The same result should follow here.

3. California Law Precludes a Finding that LiveRamp's Conduct Is Highly Offensive.

Ultimately, Plaintiffs' thesis is that aggregating data for ad delivery is inherently "highly offensive," irrespective of the quality of the disclosures, the nature of the opt-outs, or how the data is obtained. This sweeping theory cannot be reconciled with the "social norms underlying the privacy right," *Low*, 900 F. Supp. 2d at 1025, as expressed by California voters. *See Romero v. Dep't Stores Nat'l Bank*, 725 Fed. App'x 537 (9th Cir. 2018) (legislature's judgment relevant to "highly offensive" analysis). As Plaintiffs acknowledge, California has enacted comprehensive laws governing the data industry, including both the CCPA and the CPA, enacted through Proposition 24. Although Plaintiffs cite snippets referencing these laws to suggest that targeted ad delivery is *malum in se*, voters determined otherwise. In enacting Proposition 24, California voters expressly determined that "[o]ne of the most successful business models for the internet has been services that rely on advertising to make money as opposed to charging consumers," and that "[a]dvertising-supported services have existed for generations and can be a great model for consumers and businesses alike." *See* Cal. Prop. 24 (2020) § 2(I).

The voters and the Legislature did not ban data collection or deem consent impossible. (*See* Compl. ¶¶ 129-143.) They did not even require affirmative consent for data collection. Instead, they enacted a regime that balanced the competing interests in privacy and access to a free and open internet by requiring registration of data brokers, mandating point-of-collection

disclosures, limiting data collection, creating easy-to-use opt-*out* and correction mechanisms, among other safeguards. Cal. Civil Code §§ 1798.100 *et seq.* Plaintiffs ask the Court to upend this "balance" by substituting their policy preferences for those expressed by the voting majority who that approved Prop 24. This should not be permitted. California voters' decision to regulate the collection of consumer information rather than banning the practice outright establishes that LiveRamp may appropriately buy, sell, analyze, and aggregate data *without* such being treated as an "egregious breach of the social norms." *Cf. Facebook*, 956 F.3d at 606 (citation omitted).

4. Plaintiffs' Claims About Data Marketplace Fare No Better.

To the extent Plaintiffs assert invasion of privacy claims based on the operation of LiveRamp's Data Marketplace, those claims also fail. Data Marketplace permits third parties to collect, package, and market data. There is no well-pleaded allegation that *LiveRamp* sells any data, as opposed to operating a platform where data can be sold by others. (Compl. ¶ 101.) Operating a platform does not amount to a privacy violation. Even if it could, it cannot be a "highly offensive" violation because, California law expressly contemplates the existence of a market in consumer data. *See* Cal. Civil Code § 1798.100(d) ("General Duties" for "[a] business that collects a consumer's personal information and [] sells . . . or shares it with a third party"). In any event, there are no allegations about how that data was collected or processed by the sellers, what data was used to create segments, or what notice, choice, and consent options were given to users. As such, and for all the reasons stated above, Plaintiffs have not pleaded a privacy violation.

But even if Plaintiffs have pleaded a privacy violation, Section 230 of the Communications Decency Act exempts LiveRamp from liability. Section 230 immunizes providers of interactive computer services against liability arising from third-party content. It provides that "No provider ... of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider." 47 U.S.C. § 230(c). An "interactive computer service" is an "expansive" term that covers "*any* . . . service . . . that *provides or enables computer access by multiple users to a computer server*." *In re Zoom Video Commc'ns Inc. Priv. Litig.*, 525 F. Supp. 3d 1017, 1029 (N.D. Cal. 2021) (quoting 47

U.S.C. § 230(f)(2) and holding that Zoom is an "interactive computer service"). Courts have found that online marketplaces like Amazon fall within that definition, and the reasoning applies equally to LiveRamp's Data Marketplace. *See Lee v. Amazon.com, Inc.*, 76 Cal. App. 5th 200, 251 (Ct. App. 2022). Section 230 precludes liability for "any cause of action that would make service providers liable for information originating with a third-party user of the service." *Perfect 10, Inc. v. CCBill LLC*, 488 F.3d 1102, 1118 (9th Cir. 2007) (cleaned up).

Courts interpret Section 230 "expansively," *Dyroff v. Ultimate Software Grp., Inc.*, 934 F.3d 1093, 1097 (9th Cir. 2019), as barring "a panoply of torts." *Asia Econ. Inst. v. Xcentric Ventures LLC*, 2011 WL 2469822, at *7 (C.D. Cal. May 4, 2011). As the Ninth Circuit has explained, "*any activity* that can be boiled down to deciding whether to exclude material that third parties seek to post online is perforce immune under section 230." *Fair Hous. Council of San Fernando Valley v. Roommates.Com, LLC*, 521 F.3d 1157, 1170-71 (9th Cir. 2008) (emphasis added). Consistent with this broad application, courts have enforced Section 230 as a bar to claims for invasion of privacy, *Lloyd v. Facebook, Inc.*, 2022 WL 4913347, at *7 (N.D. Cal. Oct. 3, 2022), and claims that online marketplaces should have exercised different choices about what to offer—which is precisely Plaintiffs' theory here. *See Planet Green Cartridges, Inc. v. Amazon.com, Inc.*, 2023 WL 8943219, at *5 (C.D. Cal. Dec. 5, 2023) (Amazon immune under Section 230 because "Defendants cannot be held liable for third-party content merely because it resold third-party products and re-posted third-party content").

This is a quintessential case of Section 230 protection, because Plaintiffs seek to hold LiveRamp liable for its role "as the publisher or speaker of any information provided by another information content provider." 47 U.S.C. § 230(c). Plaintiffs state in no uncertain terms that "LiveRamp's Data Marketplace provides a platform for hundreds of third-party data brokers" and yet they seek to hold LiveRamp liable for failing to prevent those third parties from posting certain content on LiveRamp's online marketplace. (*E.g.*, Compl. ¶¶ 59, 99.) Accordingly, any claim relating to the Data Marketplace is barred by Section 230 as a matter of law. *See also La Park La Brea A LLC v. Airbnb, Inc.*, 285 F. Supp. 3d 1097, 1106 (C.D. Cal. 2017).

B. Plaintiffs Fail to State a Claim Under CIPA or the ECPA (Counts III & IV).

Plaintiffs do not plausibly allege that LiveRamp's practices violate CIPA or ECPA. (Compl. ¶¶ 185-237.) Both claims address LiveRamp's alleged use of "Client-Side Tags" and "Enhanced Client-Side Tags." These tools allegedly use "pixels" to collect browsing data. (*Id.* ¶¶ 77, 89.) Plaintiffs allege that this software is an unlawful form of interception under ECPA and CIPA Section 631(a) and that it constitutes an unlawful "pen register" in violation of CIPA Section 638.51. Practically speaking, these claims amount to an assertion that much of the internet is illegal. Plaintiffs fail to state a claim as a matter of law.

1. Plaintiffs' CIPA Section 631(a) and ECPA Interception Claims Fail.

To plead an interception claim under the ECPA, Plaintiffs must allege that LiveRamp "(1) intentionally (2) intercepted (3) the contents of (4) plaintiffs' electronic communications (5) using a device." *In re Meta Pixel Healthcare Litig.*, 647 F. Supp. 3d 778, 794–95 (N.D. Cal. 2022). "The analysis for a violation of CIPA is the same as that under the federal Wiretap Act." *Brodsky v. Apple Inc.*, 445 F. Supp. 3d 110, 127 (N.D. Cal. 2020). Plaintiffs' interception claims fail for two standalone reasons: (1) the ECPA is a one-party consent statute and LiveRamp's clients installed its tools and (2), Plaintiffs do not plausibly allege interception "in transit."

a. LiveRamp's Clients Consented to Any Alleged Interception.

Plaintiffs' ECPA claim must be dismissed because the ECPA is a one-party consent statute. 18 U.S.C. § 2511(2)(d). Absent inapplicable exceptions here, it is not unlawful to intercept a communication when "one of the parties to the communication has given prior consent[.]" *Id.* Here, the Complaint alleges only that the LiveRamp pixel operates on websites of LiveRamp clients who have chosen to enable it. (Compl. ¶¶ 189, 192.) There are no allegations that LiveRamp's pixel operates on websites without the consent of the operator. (Compl. ¶¶ 185-202.) Indeed, the name says it all: a ***client****-side tag.*

Courts have dismissed ECPA interception claims based on similar allegations. In *Katz-Lacabe*, 668 F. Supp. 3d 928, plaintiffs alleged that Oracle collected digital identifiers using "tracking pixels (code embedded into webpages that track information whenever the webpage is opened)." *Id.* at 935-36. The court dismissed the ECPA interception claim, reasoning that

because "Defendant's customers must have chosen to deploy Oracle's tools on their websites, it necessarily follows that 'one of the parties to the communication'—the websites themselves—gave 'prior consent to such interception.'" *Id.*at 945. The same result must follow here.[12]

b. Plaintiffs Cannot Allege an Interception "In Transit."

Plaintiffs' ECPA and CIPA interception claims fail on a separate basis because Plaintiffs have not plausibly alleged that LiveRamp intercepted the contents of a communication while it was "in transit," which is an essential element of both claims. *See Adler v. Community.com, Inc.*, 2021 WL 4805435, at *4 (C.D. Cal. Aug. 2, 2021). This element requires a showing that the contents were "acquired *during transmission*, not while it is in electronic storage." *Konop*, 302 F.3d at 878 (emphasis added). If LiveRamp received communications *after* the websites received them, any alleged interception was not "during transmission," no matter how quickly thereafter. *Griffith v. TikTok, Inc.*, 2024 WL 5279224, at *10 (C.D. Cal. Dec. 24, 2024).

Here, Plaintiffs plead no facts to support their conclusory assertion that LiveRamp's pixel intercepts communications "in transit." (Compl. ¶ 189.) Plaintiffs' "formulaic recitation of the elements" of their interception claim is no substitute for plausible factual allegations establishing how the interception in transit allegedly occurs. *See Twombly*, 550 U.S. at 555.

Moreover, facts that are alleged (sparse as they are) are logically inconsistent with interception in transit. Plaintiffs allege that LiveRamp's pixel intercepted "detailed URLs of webpages Plaintiff Riganian viewed" including URLs "revealing searches she performed." (Compl. ¶ 193.) But LiveRamp could not plausibly have intercepted Plaintiffs' inputs into websites (for instance, search terms typed into a search bar) before those websites returned URLs reflecting what those inputs were. This is logically impossible under the "protocol govern[ing] how communications occur between 'clients' and 'servers,'" as summarized in *In re Zynga Privacy Litigation*, 750 F.3d 1098, 1101 (9th Cir. 2014). As the Ninth Circuit explained, "when

[12] The statute's "crime-tort" exception" does not apply to a case "where Defendant's 'purpose has plainly not been to perpetuate torts on millions of Internet users, but to make money." *Katz-Lacabe*, 668 F. Supp. 3d at 936. Plaintiffs allege that LiveRamp's primary motivation for all of its conduct was for profit. (*See* Compl. ¶ 1 ("LiveRamp uses its systems to *profit* from Americans' nearly every move online and offline, selling that information to third parties so that they may further surveil and manipulate people."); *see also* ¶¶ 110, 235, 241.)

users enter URL addresses into their web browser . . . they are actually telling their web browsers (the client)" to send a "GET request" asking to load a particular webpage. *Id*. at 1102. The website, *i.e.* the "server," responds to the GET request by "retrieving" the "requested information or content," typically a webpage, from where it is hosted and relaying the associated URL. *Id.* at 1101. Thus, the only way that LiveRamp could receive information from Plaintiffs' URLs—*e.g.*, "page views," "ad views," or "adding items to cart" (Compl. ¶¶ 77, 189)—is *after* Plaintiffs' web browsers (the "clients") sent Plaintiffs' "GET" request to whatever website they visited and received the website's response. *Id*. Because LiveRamp could not have received Plaintiffs' communications to websites until ***after*** the websites received them, Plaintiffs have no ECPA or CIPA section 631(a) claim. *See Griffith*, 2024 WL 5279224, at *10 ("sequence" is determinative for interception claims).

2. Plaintiffs Fail to Plausibly Allege that LiveRamp Operated an Illegal "Pen Register" in Violation of CIPA Section 638.51.

Plaintiffs' CIPA Section 638.51 claim (Compl. ¶¶ 203-219) fails because Plaintiffs have not plausibly alleged that LiveRamp's Client-Side Tags and Enhanced Client-Side Tags are unlawful "pen registers." Plaintiffs' theory cannot be squared with the relevant statutory text, the legislative history, or the applicable canons of construction. Indeed, if adopted, Plaintiffs' approach would effectively criminalize much of the internet.

The California Legislature enacted the pen register provision in 2015 through Assembly Bill 929 ("AB 929").[13] That Bill codified procedures governing the use of pen registers by law enforcement and prohibited the use of pen registers without a court order, subject to several exceptions. Cal. Penal Code § 638.51(a). The Bill defined "pen register" as "a device or process that records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, but not the contents of a communication." Cal. Penal Code § 638.50(b). Although the internet was

[13] *See* A.B. 929, 2015-2016 Leg., 16th Sess. (Cal. 2015), (hereinafter "A.B. 929"), Templeton Decl. Exhibit C.

widespread by the time the law was enacted, neither the statutory text nor the legislative history targeted tracking or recording activity on the internet.

Other sections of the statutory text—which were enacted into law at the same time as the provision prohibiting pen registers without a court order—make clear that the law was intended to apply to devices used for *telephone* surveillance only: Penal Code Section 638.52(c) provides that a pen register may not collect the physical location of the subscriber "except to the extent that the location may be determined *from the telephone number*." *Id*. (emphasis added). Section 638.52(d) also states that any court order authorizing law enforcement to use a pen register must identify the person associated with the "*the telephone line to which the pen register ... is to be attached*." *Id.* (emphasis added). The legislative history is to the same effect. *See Day v. City of Fontana*, 25 Cal. 4th 268, 272 (2001) ("legislative history" to construe ambiguous statutes). The author's note to Assembly Bill 929 equated pen registers with telephonic technology, explaining that pen registers "allow[] law enforcement officers to record all outgoing numbers *from a particular telephone line*." *See* A.B. 929 at 15 cmt.1 (Cal. June 15, 2015) (emphasis added), available at Templeton Decl. Exhibit A at 8. Another committee report also described pen registers in telephonic terms. *See* A.B. 929 at cmt. 2 (Cal. Apr. 7, 2015), available at Templeton Decl. Exhibit D at 10 ("Pen registers … generally track *incoming and outgoing telephone calls*." (emphasis added)). As one court noted in dismissing a pen register claim based on internet tracking software, the "pen register" definition references technology from "an era of cordless radio phones and cellular phones." *Licea v. Hickory Farms LLC*, 2024 WL 1698147, at *2 (Cal. Super. Ct. Mar. 13, 2024).

If there was any doubt, that doubt is resolved by the rule of lenity. The prohibition on "pen registers" appears within a penal statute codified in the Penal Code. And when it comes to criminal statutes, "the defendant must be given the benefit of every reasonable doubt as to whether the statute applies to him." *Sanchez v. Cars.com Inc.*, 2025 WL 487194, at *3 (Cal. Super. Ct. Jan. 27, 2025) (interpreting "pen register"); *In re Zerbe*, 60 Cal. 2d 666, 668 (1964).

The statute's text and the repeated references to telephonic communications in the legislative history make clear that CIPA's pen register provision was not intended to criminalize

software that reveals web browsing activity. A contrary interpretation would outlaw a wide and indeterminate range of online activity that the Legislature never contemplated.

For these reasons, a growing body of cases have held that CIPA's pen register provisions do not apply to tracking on to the internet. In *Sanchez*, the California Superior Court held that software embedded in a website that "capture[d] outgoing information" from visitors and transmitted it to a third-party (for use in ad campaigns) was not a pen register. 2025 WL 487194, at *2. The court reasoned that the legislative history confirmed that the Legislature did not intend CIPA's pen register provision to apply to internet tracking software, only telephonic activity. *Id.* at *3. Similarly, in *Licea*, another Superior Court dismissed a CIPA claim alleging that an online retailer violated CIPA's pen register provision by capturing the plaintiff's IP address when the plaintiff visited its website. 2024 WL 1698147, at *4. The court found that the plaintiff's broad application of the pen register provision to encompass online communications would "potentially disrupt a large swath of internet commerce without further refinement as the precise basis of liability." *Id.*

While two federal judges have declined to dismiss software-based "pen register" claims at the pleading stage, neither court addressed the arguments favoring a narrower construction that LiveRamp advances here. *See Shah v. Fandom, Inc.*, 2024 WL 4539577, at *3 (N.D. Cal. Oct. 21, 2024); *Zarif v. Hwareh.com, Inc.*, 2025 WL 486317, at *4 (S.D. Cal. Feb. 13, 2025) (Bashant, J.); *Greenley v. Kochava, Inc.*, 684 F. Supp. 3d 1024, 1050 (S.D. Cal. 2023) (Bashant, J.). None addressed the rule of lenity which *requires* narrow interpretations of criminal statutes to protect due process rights, and only one of these decisions considered (in a brief footnote) any legislative history materials. That is presumably why more recent decisions have deemed these earlier decisions unpersuasive. *See Sanchez*, 2025 WL 487194, at *3.

C. Plaintiffs Cannot Bring a Standalone Unjust Enrichment Claim (Count V).

Plaintiffs fail to plead the elements of unjust enrichment. "To allege unjust enrichment as an independent cause of action, a plaintiff must show that a defendant received and unjustly retained a benefit at the plaintiff's expense." *Russell v. Walmart, Inc.*, 680 F. Supp. 3d 1130, 1133 (N.D. Cal. 2023) (Tigar, J.) (citation omitted). Plaintiffs must allege "mistake, fraud,

coercion, or request" by LiveRamp and that Plaintiffs conferred a benefit on LiveRamp that would be unjust for it to retain. *Id*. Plaintiffs conclusorily allege that LiveRamp's "unauthorized use" of their "information for profit entitles them to profits unjustly earned." (Compl. ¶ 251.) But they do not explain, as they must, how LiveRamp's conduct rises to the level of mistake, fraud, coercion, or request. *See Russell*, 680 F. Supp. 3d at 1133 (dismissing unjust enrichment claim when plaintiff alleged that self-checkout "customers confer a benefit on Walmart when providing uncompensated labor").

In *Katz-Lacabe*, the court dismissed an unjust enrichment claim pled under a similar theory. *See Katz-Lacabe*, 668 F. Supp. 3d at 946 (plaintiffs "were at no time in direct privity" with defendant and "have neither directly expended their own resources, nor shown that their property has become less valuable"). The court explained that where, as here, "Plaintiffs challenge unjust enrichment based on the monetization of th[e] data" that the defendant "received and/or collected with permission from the third-party websites," the plaintiffs "must explain why the access they received to those websites would not defeat the unjust enrichment claim." *Id*. n.11. This Court should similarly dismiss Plaintiffs' unjust enrichment claim.

D. Plaintiffs' Duplicative Claim for Declaratory Judgment Fails (Count VI).

Plaintiffs' declaratory judgment claim (Compl. ¶¶ 256–59) should be dismissed because the Declaratory Judgment Act "does not provide an independent theory for recovery." *Hammerling*, 615 F. Supp. 3d at 1097 (citation omitted). Declaratory relief is unavailable "if the underlying claims are dismissed." *Id.* Because the rest of Plaintiffs' claims must be dismissed for failure to state a claim, the Court should dismiss Plaintiffs' Sixth Cause of Action as well.

V. CONCLUSION

For the foregoing reasons, all claims against LiveRamp should be dismissed.

Dated: March 28, 2025

WILSON SONSINI GOODRICH & ROSATI
Professional Corporation

By:/s/ *Matthew A. Macdonald*
Matthew A. Macdonald
E-mail: matthew.macdonald@wsgr.com

Attorney for Defendant
LIVERAMP HOLDINGS, INC.